

## CLAIMS

What is claimed is:

1           1. A multi-word arithmetic device for executing modular  
2 arithmetic on multi-word integers, in accordance with  
3 instructions from an external device, the multi-word  
4 arithmetic device comprising:

5           a memory;

6           an arithmetic unit for executing, on word units, at least  
7 two types of calculation, including addition and  
8 multiplication, and outputting a one-word calculation result;

9           a memory input/output circuit for performing (1) a first  
10 data transfer for storing in the memory at least one integer  
11 received from an external device, (2) a second data transfer  
12 for inputting at least one integer stored in the memory into  
13 the arithmetic unit in word units, (3) a third data transfer  
14 for storing in the memory the calculation result output from  
15 the arithmetic unit, and (4) a fourth data transfer for  
16 outputting the calculation result from the memory to the  
17 external device; and

18           a control circuit for, according to instructions received  
19 from the external device,

20           (a) specifying, to the memory input/output unit, data to

21 be transferred by the second and third data transfers, and

22 (b) specifying, to the arithmetic unit, a type of  
23 calculation to be executed,

24 thereby controlling:

25 (i) the arithmetic unit to selectively perform one of at  
26 least two types of modular arithmetic on the at least one  
27 integer stored in the memory; and

28 (ii) the memory input/output circuit to store the  
29 calculation result of the modular arithmetic into the memory.

1 2. The multi-word arithmetic device of Claim 1, wherein  
2 at least two integers are stored in the memory,  
3 the arithmetic unit includes:

4 an adder for adding at least two pieces of one-word data;

5 and

6 a multiplier for multiplying at least two pieces of one-  
7 word data, and

8 the memory input/output circuit simultaneously reads one  
9 word from each of the at least two integers stored in the  
10 memory, and outputs the read words to one of the adder and the  
11 multiplier.

1 3. The multi-word arithmetic device of Claim 2, wherein:

2 the memory is divided into two dual-port memories, each  
3 allowing access to two storage areas designated by two  
4 addresses, and allowing (1) two read operations, or (2) one  
5 read operation and one write operation to be performed  
6 simultaneously on word units; and

7 the at least two integers are stored in each dual-port  
8 memory so that the memory input/output circuit can  
9 simultaneously (1) read a piece of one-word data  
10 simultaneously from each of the integers stored in the two  
11 dual-port memories, and have the read pieces of data input  
12 into one of the adder and the multiplier, and (2) write a  
13 piece of one-word data output from one of the adder and the  
14 multiplier into one of the two dual-port memories.

1 4. The multi-word arithmetic device of Claim 1, wherein  
2 the arithmetic unit, according to instructions from the  
3 control circuit, executes one of the following three  
4 calculations: (1) addition of at least two pieces of one-word  
5 data; (2) multiplication of two pieces of one-word data; and  
6 (3) multiplication of two pieces of one-word data and  
7 accumulation of multiplication results.

1 5. The multi-word arithmetic device of Claim 4, wherein

2 the arithmetic unit includes:

3 a multiplier receiving an input of two pieces of one-word  
4 data and outputting a piece of two-word data;

5 an adder receiving an input of at least two pieces of two-  
6 word data, including a piece of two-word data output from the  
7 multiplier, and outputting a piece of multi-word data; and

8 a selecting circuit selecting, according to instructions  
9 from the control circuit:

10 (1), data to be input into one of the multiplier and the  
11 adder out of data transmitted from the memory input/output  
12 circuit; and

13 (2) data to be output as the calculation result out of data  
14 output from one of the adder and the multiplier.

1 6. The multi-word arithmetic device of Claim 1, wherein  
2 the at least two types of modular arithmetic include modular  
3 addition, and

4 on receiving, from the external device, an instruction to  
5 execute modular addition and an indication of a number of  
6 words  $n$  for each integer on which modular addition is to be  
7 performed, the control circuit controls the memory  
8 input/output circuit and the arithmetic unit to execute the  
9 following processing:

10 (1) the memory input/output circuit obtains from the  
11 external device and stores in the memory two  $n$ -word integers  $A$   
12 and  $B$  on which modular addition is to be executed and a  $n$ -word  
13 integer  $P$  showing a modulus;

14 (2) the memory input/output circuit (a) reads  
15 simultaneously, from the integers  $A$ ,  $B$  and  $P$  stored in the  
16 memory, pieces of one-word data  $a$ ,  $b$  and  $p$ , each with a same  
17 digit position, and has the read pieces of data input into the  
18 arithmetic unit, while (b) storing in the memory a piece of  
19 one-word data  $w$  output from the arithmetic unit, and repeats  
20 processes (a) and (b) sequentially from a lowest-order word in  
21 each integer until  $n$  words of data are obtained, enabling an  
22  $n$ -word integer  $W$  to be stored in the memory; and

23 (3) the arithmetic unit repeats  $n$  times a process in which  
24 the pieces of data  $a$ ,  $b$  and  $p$  received from the memory  
25 input/output circuit are computed as  $a + b - p$ , propagating a  
26 carry, and a result  $w$  is output.

1 7. The multi-word arithmetic device of Claim 6, wherein  
2 the control circuit determines whether a carry has been  
3 generated by the arithmetic unit immediately after completion  
4 of the processing (1) to (3) and if a carry has been  
5 generated, further controls the memory input/output circuit

6 and the adder to execute the following processing:

7 (4) the memory input/output circuit (a) reads  
8 simultaneously, from the integers  $W$  and  $P$  stored in the  
9 memory, pieces of one-word data  $w$  and  $p$ , each with a same  
10 digit position, and has the read pieces of data input into the  
11 arithmetic unit, while (b) storing in the memory a piece of  
12 one-word data  $c$  output from the arithmetic unit and repeats  
13 processes (a) and (b) sequentially from a lowest-order word in  
14 each integer until  $n$  words of data are obtained, enabling an  
15  $n$ -word integer  $C$  to be stored in the memory; and

16 (5) the arithmetic unit repeats  $n$  times a process in which  
17 the pieces of data  $w$  and  $p$  received from the memory  
18 input/output circuit are computed as  $w + p$ , propagating a  
19 carry, and a result  $c$  is output.

1 8. The multi-word arithmetic unit of Claim 1, wherein the  
2 at least two types of modular arithmetic include Montgomery  
3 reduction calculating a residue for  $A \cdot R^{-1} \bmod P$ , when each  
4 word has  $k$  bits,  $A$  is a  $2n$ -word integer used for input data,  $R$   
5 is an integer  $2^{(k \times n)}$  and  $P$  is an  $n$ -word integer; and

6 upon receiving, from the external device, an instruction to  
7 execute Montgomery reduction and an indication of a number of  
8 words  $2n$  for an integer  $A$  on which Montgomery reduction is to

9 be performed, the control circuit controls the memory  
10 input/output circuit and the arithmetic unit to execute  
11 Montgomery reduction.

1 9. The multi-word arithmetic device of Claim 8, wherein,  
2 when receiving an instruction to execute Montgomery reduction  
3 from the external device, the control circuit controls the  
4 memory input/output circuit and the arithmetic unit so as to  
5 execute the following processing:

6 (1) the memory input/output circuit acquires integers A, P  
7 and V from the external device and stores the obtained  
8 integers in the memory, the integer V being  $-P^{(-1)} \bmod R$ ;

9 (2) the arithmetic unit computes partial products for words  
10 from each of (i) a lower  $n$  words of the integer A stored in  
11 the memory, and (ii) the integer V, and accumulates words in  
12 partial products having a same digit position, repeating the  
13 process sequentially from a lowest word in each integer until  
14  $n$  words of accumulated results are obtained, and storing the  
15 accumulated results in the memory as a piece of  $n$ -word  
16 intermediate data B;

17 (3) the arithmetic unit computes partial products for words  
18 from each of (a) the piece of intermediate data B and (b) the  
19 integer P stored in the memory, and accumulates words in the

20 partial products having a same digit position so that, when a  
21 lowest word is a 0th word, accumulated results for a 0th to  
22  $(n-3)$ th word are not obtained, but accumulated results for a  
23  $(n-2)$ th word to a  $(2n-1)$ th word are obtained and stored in the  
24 memory as the upper  $(n+1)$  words of a piece of intermediate  
25 data D;

26 (4) the arithmetic unit (a) generates (i) a carry obtained  
27 from a one-word addition performed by adding a lowest word  
28 from each of the piece of intermediate data D and an integer  
29 AA, and (ii) a one-bit logical value, the integer AA being an  
30 upper  $(n+1)$  words of the integer A, and the one-bit logical  
31 value being 0 when a one-word addition result is 0, and 1 when  
32 the one-word addition result is not 0, and (b) adds an upper  $n$   
33 words of the piece of intermediate data D, an upper  $n$  words of  
34 the integer AA, the carry and the one-bit logical value, by  
35 repeating addition of word units sequentially from a lowest  
36 word in each integer, while propagating a carry, until  $n$  words  
37 of data are obtained, and stores an addition result in the  
38 memory as a piece of  $n$ -word output data M; and

39 (5) when the output data M stored in the memory is at least  
40 as large as the integer P, the arithmetic unit subtracts the  
41 integer P from the output data M until the output data M is 0  
42 or a positive integer smaller than the integer P, by repeating

43 subtraction of word units sequentially from a lowest word in  
44 each integer, while propagating a carry, until  $n$  words of data  
45 are obtained, and stores the subtraction results in the memory  
46 as a new piece of  $n$ -word output data  $M$ .

1 10. The multi-word arithmetic device of Claim 9, wherein  
2 in processing (4), the arithmetic unit adds a piece of one-  
3 word data containing all ones to the piece of intermediate  
4 data  $D$  and the integer  $AA$ , and stores an upper  $n$  words of an  
5 obtained addition result in the memory as the output data  $M$ .

1 11. The multi-word arithmetic device of Claim 10, wherein,  
2 in processing (2) and (3), the arithmetic unit selects sets of  
3 word pairs, each set formed from all the pairs of words that  
4 generate a partial product with a same digit position, sets  
5 input values in the multiplier, and computes and accumulates  
6 the partial products for the selected pairs of words in  
7 sequence from the set with a lowest digit position.

1 12. The multi-word arithmetic device of Claim 11, wherein,  
2 in processing (2) and (3), the arithmetic unit stores in the  
3 memory as part of a multiplication result a lower word from a  
4 two-word accumulated result obtained by accumulating partial

5 products with the same digit position, and adds an upper word  
6 from the accumulated result to partial products that have a  
7 digit position one word higher and are thus the next to be  
8 calculated.

1 13. The multi-word arithmetic device of Claim 12, wherein  
2 the arithmetic unit performs an operation for storing a lower  
3 word from the accumulated result in the memory simultaneously  
4 with an operation for adding an upper word from the  
5 accumulated result to partial products that have a digit  
6 position one word higher and are thus the next to be  
7 calculated.

1 14. The multi-word arithmetic device of Claim 10, wherein,  
2 when computing and accumulating partial products in processing  
3 (2) and (3), the arithmetic unit updates accumulated values by  
4 (a) simultaneously (i) computing a partial product and (ii)  
5 reading a previously accumulated one-word value from the  
6 memory, (b) adding the accumulated one-word value to a  
7 corresponding word in the partial product, and (c) storing a  
8 result of the addition in a corresponding area of the memory.

1 15. A multi-word arithmetic device for executing modular

2 arithmetic on multi-word integers, in accordance with  
3 instructions from an external device, the multi-word  
4 arithmetic device comprising:

5 a memory;

6 an arithmetic unit for executing, on word units, at least  
7 two types of calculation, including addition and  
8 multiplication, and outputting a one-word calculation result;

9 a memory input/output circuit for performing (1) a first  
10 data transfer for storing in the memory at least one integer  
11 received from an external device, (2) a second data transfer  
12 for inputting at least one integer stored in the memory into  
13 the arithmetic unit in word units, (3) a third data transfer  
14 for storing in the memory the calculation result output from  
15 the arithmetic unit, and (4) a fourth data transfer for  
16 outputting the calculation result from the memory to the  
17 external device; and

18 a control circuit for, according to instructions received  
19 from the external device,

20 (a) specifying, to the memory input/output unit, data to  
21 be transferred by the second and third data transfers, and

22 (b) specifying, to the arithmetic unit, a type of  
23 calculation to be executed,

24 thereby controlling:

(i) the arithmetic unit to selectively perform one of at least two types of modular arithmetic on the at least one integer stored in the memory; and

(ii) the memory input/output circuit to store the calculation result of the modular arithmetic into the memory,

wherein the at least two types of modular arithmetic include modular addition and Montgomery reduction; and

the control circuit controls the memory input/output

circuit and the arithmetic unit so that the arithmetic unit

(1) computes  $A+B \bmod P$  when an instruction for executing

modular addition is received from the external device,  $A$ ,  $B$

and  $P$  being  $n$ -word integers, and (2) computes a residue for  $A \cdot$

$R^{-1} \bmod P$ , when an instruction for executing Montgomery

reduction is received from the external device, each word

having  $k$  bits,  $A$  being a  $2n$ -word integer used as input data,  $R$

being an integer  $2^{(k \times n)}$  and  $P$  being an  $n$ -word integer.

16. The multi-word arithmetic unit of Claim 15, wherein the arithmetic unit includes:

a multiplier receiving an input of two pieces of one-word data and outputting a piece of two-word data;

an adder receiving an input of at least two pieces of two-word data, including a piece of two-word data output from the

multiplier, and outputting a piece of multi-word data; and  
a selecting circuit selecting, according to instructions  
from the control circuit:

(1), data to be input into one of the multiplier and the  
adder out of data transmitted from the memory input/output  
circuit; and

(2) data to be output as the calculation result out of data  
output from one of the adder and the multiplier.

17. The multi-word arithmetic unit of Claim 16, wherein  
the memory is divided into two dual-port memories, each  
allowing access to two storage areas designated by two  
addresses, and allowing (1) two read operations, or (2) one  
read operation and one write operation to be performed  
simultaneously on word units; and

the at least two integers are stored in each dual-port  
memory so that the memory input/output circuit can  
simultaneously (1) read a piece of one-word data  
simultaneously from each of the integers stored in the two  
dual-port memories, and have the read pieces of data input  
into one of the adder and the multiplier, and (2) write a  
piece of one-word data output from one of the adder and the  
multiplier into one of the two dual-port memories.